REMARKS

Upon entry of this amendment, Claims 15-47 will be pending in this application. In view of the foregoing amendments and the following remarks, applicant respectfully requests consideration of the new Claims.

New Claims 15-47 are not anticipated or made obvious by, and further differentiate the claimed invention over the prior art of record. The biggest difference between the current invention and all others is that the user authentication data is used to form the key that is used to encrypt all data whereas, all other inventions use the encrypted authentication data for subsequent authentication. Elements that contribute to the Claims' novelty include, but are not limited to, the following.

Claim 15 recites the delivery of the encrypt/decrypt engine via a web page, encryption independent from the identity of the client. Ross requires dependence on the identity of the physical client. In the current invention, the encryption key is derived from the user of the client and not the physical client.

Claim 16 recites that the encryption key in the current invention is entered by the user and is independent of the identity of the physical client. Because there may be the possibility to confuse the physical

client identity and the user client identity, clarification has been made herein. It is quite clear from Fig. 8 that the invention has always been with respect to the user of the client and not the physical client itself.

Claim 17 recites delivery of stored data responsive to completion of a processing step.

Claim 18 recites storage of encrypted data followed by delivery of the stored data responsive to a request from either the original client or another client.

Claim 19 recites lower limits on the number of times a key must be transmitted. The crux of the invention is embodied herein, in that a de facto authentication takes place, because while the authentication information is not sent, the server can determine exactly the source of the data if and only if it can in fact decrypt the data. No prior art can be found where the authentication is tied explicitly to the ability to decrypt an encrypted text and not to a comparison of user identification tokens (username and password for example). Consequently, the shared key is only sent to the server one time and may never be sent to the client.

Laursen et al, (6,065,120) have a similar strategy, but in fact they utilize information about the user base on the client. The authentication and subsequently the encryption/decryption is tied to whether the user can identify themselves based on information that is transmitted.

Additionally, they explicitly state that the invention that we have here is excluded intentionally by their invention (page 3, line 1). Our invention, renders the username and password strong and is thus diametrically opposite to what they have invented.

Bodnar (6,061,790) proposes a system wherein two different keys are required for logging in and transmitting data. Additionally, Bodnar requires the client (page 10, last paragraph) to make use of client hardware to generate the encryption key. It would not be a trivial exercise to get our invention from this patent. Again. Bodner is concerned only with the transmission of ones own transmissions. We are of the opinion that it would be impossible to utilize Bodnar to send and receive email without the use of public/private key pairs that would need to be distributed. Also, it is clear from both Bodner and Ross, that identifying information on the server is used to authenticate and thus initiate the session (Bodner page 10 line 10, for example)

Claim 22 recites an encrypt/decrypt engine configured to operated independently of the identity of the physical client.

Claim 23 recites decryption and re-encryption of the data using a key of the server.

Claim 24 recites encryption of data for delivery responsive to the completion of a processing step. The encryption using the shared key or another shared key. Delivery may be to the client or another client.

Claim 25 is similar to Claim 24 except that operation is responsive to a request for the data.

Claims 25 and 26 include two possibilities for the source of a request for data.

Claim 28 recites the restriction of storage, of all data entered by the user on the client, to storage in encrypted form. Claim 28 also recites use of a key entered by the user for encryption.

Claim 29 recites use of a symmetric key.

Claim 31 is a method claim reciting use of a web page to deliver the encrypt/decrypt engine and reciting use of a shared key entered by a user.

Claims 32-36 include various methods of processing the data receive at the server.

Claims 37-41 recites a computer-readable medium comprising program instructions. The program instructions may execute methods of the invention possibly using the systems of the invention.

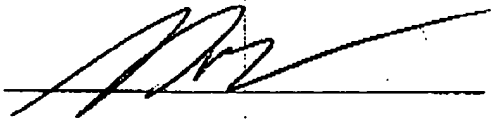
Claim 43 is a method claim including encryption of data independently of an identity of the physical client using a shared key entered by a user. Here it must be explicitly understood that the client is the device that communicates with a server, whereas, the user is the actual entity causing the client to perform work. Claim 43 clarifies the novelty because the user is not tied to a specific client and, the encryption and data delivery is tied to the user and not the physical client.

Claim 44- 47 include further details of the step of processing data decrypted at the server.

Conclusion

In specifying the invention, the Applicant has reviewed the prior art of Krajewski (5,590,199), Linehan (5,495,533), Diffie et al (5,371,794), Wobber et al (5,235,642), Lennon et al (4,193,131), Barnes et al (5,970,475), Smithies et,al (6,091,835), Ross (5,812,671) and others. None of these would preclude the current invention from being allowed.

The Applicant respectfully request a Notice of Allowability. If the Examiner has questions regarding the case, the Examiner is invited to contact Applicant's undersigned representative at the number given below.

Dated: September 2, 2003 By: 

Lynn D. SPraggs, Ph.D.
Ultra Information Systems Inc.
2179 11th Ave.
Vernon BC Canada
V1T 8V7
Tel: (250) 542-0112
Fax: (250) 549-3751
Email: lspraggs@uisamerica.com

Appendix showing changes to the Specification.

Replace the paragraph beginning on page 6 line 14 with:

Referring now to FIG. 1, a schematic diagram illustrates a server 100 used to receive encrypted data from a sending client computer 102 and transmit encrypted data to a receiving client computer 104 through the Internet 106 using shared private keys. The sending client 102 and receiving client 104 share their own private key with the server 100, but do not share their private keys with anyone else.

Replace the paragraph beginning on page 8 line 6 with:

FIG. 5 is a block diagram of one embodiment of the non-volatile memory module 404 located within the clients 102, 104 of FIG. 4. The non-volatile memory 406 includes an encrypt/decrypt engine 502 for encrypting and decrypting data. The encrypt/decrypt engine 502 can also be stored in RAM 404. Excellent results can be obtained when the encrypt/decrypt engine is served up as a Java™ applet to the clients 102, 104. The Java™ applet can be served up with a web page. In another form, the encrypt/decrypt engine can be sent to the clients 102, 104, and then stored on their hard drive. ~~The Java™ applet can be served up with a web page from an email sent to the clients 102, 104, and then stored on their hard drive.~~

Replace the paragraph beginning on page 10 line 3 with:

FIG. 8 is a flowchart of a method illustrating how a user having a shared private key passes secure data through a server computer over the Internet. This method is very similar to the process described in FIGS. 6 and 7. The process begins at step 800. A ~~client~~ user having a private key shared with the server establishes a session over the Internet with the server by requesting a web page at step 802 using a suitable client. At step 804 the server sends a web page form from the web page forms database 310 to the client. Next at step 806 the ~~client~~ user enters data into the web page along with his private key shared with the server. At step 808 the data is encrypted with the encrypt/decrypt engine at the client computer using the user's private key and then the encrypted data is sent to the server. It is explicitly shown at step 808 that the user's private key is the user's personal authentication data. The encryption key is formed from the authentication data. Subsequently, the authentication data is NOT sent to the server and it is NOT used for authentication per se except in so far as both client and server are able to encrypt and decrypt the data using the same key.

Replace the paragraph beginning on page 10 line 20 with:

After the processing step is completed at step 814 the server encrypts the processed data using the ~~client's~~ user's private key that is

stored in the user private keys database 304 and sends the encrypted data to the client. It is not necessary for the client to be the same client that began the process at step 802. The server can be used as an intermediary for passing and processing secure data between clients.

Replace the paragraph beginning on page 11 line 4 with:

At step 816, the client receives the secure data and the user enters their private key. At step 818 the encrypted processed data is decrypted with the ~~client's~~ user's private key, which is now available to the client, using the encrypt/decrypt engine 502. At step 820 the client can access the data or the user can view the data, and at step 822 the process ends.